What is claimed is:

1. A method for a network-based high-security data storage system, in which the data is stored on a server in a telecommunications network, and the local computers of the users are connected to the server over the telecommunications network,

    wherein

    -   upon request, the server operator issues to the user a user certificate for the access conditions, said user certificate being provided to the user together with a public key and a secret key, preferably on a smart card,

    -   the server accessed over the Internet sends a client program to the local computer of the user, said client program providing the user with the possibility of authentication using the smart card and transmission of further security requirements, such a biometric systems, geographic positioning, with or without time dependencies, as well as separate time restrictions, network and computer data, etc.

    -   a personal main folder is set up on the server for registered users, said main folder obtaining a special file containing the security requirements defined for this main folder as well as management information, said special file giving said main folder the status of a locker,

    -   in the main folders, further folders can be set up which are distinguished by function and which, by means of the special file containing the particular security requirements defined for them, act as functional lockers,

    -   the lockers set up in the main folders having at least the functions of personal lockers in which files can be stored only by the user of the main locker and which are only displayed to this user; provisioning lockers in which the user stores the references for files for other users in user lockers distinguished by name; receiving lockers in which the lockers of the senders of files are shown to the user, said lockers being denoted by names, and, when opening such lockers, a reference relating to the storage of the files and to the defined security requirements becomes

10

visible to the user; and public lockers, in which the user stores references to files which, when stored in the provisioning locker, are intended for a plurality of receivers, and

- the lockers are displayed only if the security-relevant requirements of the operator, user or offeror are met, so that the locker system has a virtual character.